REMARKS

Favorable reconsideration of the application is respectfully requested in light of the amendments and remarks herein. Upon entry of this amendment, claims 1-20, 39, and 71 will be pending. No new matter has been added.

In addition to the arguments presented in responses to previous office actions (which are maintained here), following additional arguments are presented.

§102 Rejection of Claims 1-6, 9-15, and 71

In Section 10 of the office action dated November 16, 2011 ("the Office Action"), claims 1-6, 9-15, and 71 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Chase et al. (U.S. Patent Pub. 2003/0135464; hereinafter referred to as "Chase").

As explained in the Manual of Patent Examination Procedure section 706.02, entitled Rejection on Prior Art, for anticipation under 35 U.S.C. 102, the reference must teach every aspect of the claimed invention either explicitly or impliedly. As is discussed below, Chase fails to teach every aspect of claims 1-6, 9-15, and 71.

Regarding independent claim 1, it recites a method of binding content to a hub network, comprising:

a) receiving a request to bind a discrete instance of content to a hub network including a single server and one or more clients as members of said hub network,

b) wherein said discrete instance includes discrete locked content data and a discrete license associated with the discrete locked content data, wherein said discrete content data and the discrete license are stored on said server,

c) wherein the discrete license is not bound to said hub network;

d) disabling said discrete instance;

e) enabling a bound instance to bind said discrete locked content data to said hub network at the server as source locked content data,

f) wherein said bound instance includes source locked content data and a root license associated with the source locked content data,

g) wherein said source content data and said root license are stored on said server, and

h) wherein said root license is bound to said hub network.

(Emphasis/reference designators added)

Before addressing each limitation of claim 1, the definition of the terms "discrete instance" and "bound instance" is addressed here. The specification recites "...disabling said discrete instance; and enabling a bound instance to bind said discrete locked content data to said hub network at the server as source locked content data." These terms are defined in at least Paragraph [0032] of the specification of the present application as published in U.S. Pub. No. 2004/0139022 and recited below (emphasis added):

> [0032] ... an instance that is compliant with hub network operation is in one of two exclusive states: discrete or bound. A discrete instance is independent of any hub network and can be played or presented through any compliant device (according to the license of the discrete instance). However, a compliant device cannot make a usable copy of a discrete instance. A discrete instance includes locked content data and a discrete license. The locked Content data of the discrete instance is referred to as the "discrete version" of the locked content data. The locked content data is locked by being protected from unauthorized access, such as by encryption. A bound instance is bound to one hub network. The bound instance

> is one logical instance represented by locked content data and corresponding licenses stored on the server of the hub network and on zero or more of the clients of the hub network. The locked content data stored by the server is the source for copies of the content data in the hub network and is the "source version." Copies of the source version content data are stored on clients and are "sub-copy versions" (though some or all of the data in the discrete version, the source version, and/or any of the sub-copy versions can be the same). A bound instance can only be played or presented through a compatible compliant device that is a member of that hub network. Members of that hub network can make sub-copies of the content data of a bound instance.

From the cited passages above, it is clear that there are two types of instances taught - discrete and bound. Discrete instances are not bound to any hub network and can be moved from one device to another using compliant media, in and out of the hub network. Additionally, compliant media will not create a copy of a discrete instance. In contrast, bound instances are bound to a single hub network. A bound instance can only be played or presented through a compatible compliant device that is a member of that hub network. Members of that hub network can make sub-copies of the content data of a bound instance.

Regarding Chase, although it alludes to content being tightly bound to a license, it fails to teach or suggest binding content to a hub network using the discrete instance of the content. Further, Chase does not teach or suggest a concept of creating a bound instance of content using discrete content, or creating a discrete instance of content from the bound content that is bound to a hub network.

Regarding limitation (a) of claim 1, it recites "receiving a request to bind a discrete instance of content to a hub network including a single server and one or more

clients as members of said hub network". Support for this limitation is found in at least Paragraphs [0033] and [0039] of the specification of the present application as published in U.S. Pub. No. 2004/0139022 and recited below (emphasis added):

> [0033] A server device can change the state of a discrete instance from discrete to bound, disabling the discrete instance and enabling a bound instance. A disabled instance is rendered unusable (e.g., through deletion or encryption of the content data of the instance or disabling the license(s) for the instance). A server device can also change the state of a bound instance from bound to discrete, disabling the bound instance (including any corresponding sub-copies) and enabling a discrete instance. In addition, the server for a hub network manages root responsibility for a bound instance. Root responsibility includes issuing and managing the licenses for the content data of the bound instance in the hub network. Accordingly, the server holds a root license defining permissions for presenting the bound instance and for managing the content data and licenses of the bound instance in the hub network. When a new sub-copy is created, a license is also created for the sub-copy from the root license. An instance of content that is not compliant with hub network operation is a non-compliant instance. A compliant device will play or copy a non-compliant instance according to whatever recognized copy control information may be associated with the instance.
>
> [0039] ... Because the instance stored on the compliant optical disc is compliant and has not been bound to any hub network yet, the instance is a discrete instance. Jim inserts the compliant optical disc into the server device of the car 120 and causes the car 120 to bind the discrete instance of the movie X to the hub network HN2. The car 120 creates a bound instance of the movie X and stores a source version of locked content data and root license as part of the bound instance in the storage of the car 120 and disables the discrete instance on the compliant optical disc (e.g., by storing data to the optical disc). After the discrete instance on the compliant optical disc has been disabled, the discrete version of the locked content data of the disabled instance cannot be played or presented on another device (as described below, in another implementation, when a

> discrete instance is bound to a hub network, the then-disabled discrete instance can still be played by member devices in the hub network to which the discrete instance was bound). In FIG. 6, the source version of the movie X is indicated by the "X" label added to the car 120. Similarly, Jim purchases and downloads a compliant instance of a song Y from network 115 and causes the car to bind the instance to the hub network HN2. In FIG. 6, the source version of the song Y is indicated by the "Y" label added to the car 120.

The Office Action cites to Chase as teaching limitation (a) in paragraphs [0144] to [0145] and [0147] to [0158], and states that these paragraphs describe "the process where DRM system **32** of user's computing device **14** performs the function of a license acquisition request to obtain a license **16** to render content **12**; see also para [0144]-[0145], where rights description in each license **16** specifies whether a user has rights to play the digital content **12** based on factors such as type of device **14** or application **34** and other information such as identification **42** of a user's computing device **14**; see also para [0186], where as part of the process of upgrading black box **30** the DRM system **32** provides hardware information unique to DRM system **32** and/or unique to user's computing device **14**; see also para [0062], where an instance is a version of digital content **12** that is unique; see also para [0109], where device **14** can be a television, monitor, dedicated audio device or a dedicated printer, among other things; see also para [0046], where a personal computer **14** can include peripherals such as a monitor **147** and a printer". The cited passages are shown below.

> [0144] As should be understood, the rights description in each license 16 specifies whether the user has rights to play the digital content 12 based on any of several factors, including who the user is, where the user is located, what type of computing device 14 the user is using, what rendering

application 34 is calling the DRM system 32, the date, the time, etc. In addition, the rights description may limit the license 16 to a pre-determined number of plays, or pre-determined play time, for example. In such case, the DRM system 32 must refer to any state information with regard to the license 16, (i.e., how many times the digital content 12 has been rendered, the total amount of time the digital content 12 has been rendered, etc.), where such state information is stored in the state store 40 of the DRM system 32 on the user's computing device 14.

[0145] Accordingly, the license evaluator 36 of the DRM system 32 reviews the rights description of each valid license 16 to determine whether such valid license 16 confers the rights sought to the user. In doing so, the license evaluator 36 may have to refer to other data local to the user's computing device 14 to perform a determination of whether the user has the rights sought. As seen in FIG. 4, such data may include an identification 42 of the user's computing device (machine) 14 and particular aspects thereof, an identification 44 of the user and particular aspects thereof, an identification of the rendering application 34 and particular aspects thereof, a system clock 46, and the like. If no valid license 16 is found that provides the user with the right to render the digital content 12 in the manner sought, the DRM system 32 may then perform the license acquisition function described below to obtain such a license 16, if in fact such a license 16 is obtainable.

[0147] DRM System 32--License Acquisition

[0148] Referring now to FIG. 7, if in fact the license evaluator 36 does not find in the license store 38 any valid, enabling license 16 corresponding to the requested digital content 12, the DRM system 32 may then perform the function of license acquisition. As shown in FIG. 3, each piece of digital content 12 is packaged with information in an un-encrypted form regarding how to obtain a license 16 for rendering such digital content 12 (i.e., license acquisition information).

[0149] In one embodiment of the present invention, such license acquisition information may include (among other things) types of licenses 16 available, and one or more Internet web sites or other site information at which one or more appropriate license servers 24 may be accessed, where each such license server 24 is in fact capable of issuing a license 16

corresponding to the digital content 12. Of course, the license 16 may be obtained in other manners without departing from the spirit and scope of the present invention. For example, the license 16 may be obtained from a license server 24 at an electronic bulletin board, or even in person or via regular mail in the form of a file on a magnetic or optical disk or the like.

[0150] Assuming that the location for obtaining a license 16 is in fact a license server 24 on a network, the license evaluator 36 then establishes a network connection to such license server 24 based on the web site or other site information, and then sends a request for a license 16 from such connected license server 24 (steps 701, 703). In particular, once the DRM system 32 has contacted the license server 24, such DRM system 32 transmits appropriate license request information 36 to such license server 24. In one embodiment of the present invention, such license 16 request information 36 may include:

[0151] the public key of the black box 30 of the DRM system 32 (PU-BB);

[0152] the version number of the black box 30 of the DRM system 32;

[0153] a certificate with a digital signature from a certifying authority certifying the black box 30 (where the certificate may in fact include the aforementioned public key and version number of the black box 30);

[0154] the content ID (or package ID) that identifies the digital content 12 (or package 12p);

[0155] the key ID that identifies the decryption key (KD) for decrypting the digital content 12;

[0156] the type of license 16 requested (if in fact multiple types are available);

[0157] the type of rendering application 34 that requested rendering of the digital content 12;

[0158] and/or the like, among other things. Of course, greater or lessor amounts of license 16 request information 36 may be transmitted to the license server 24 by the DRM system 32

> without departing from the spirit and scope of the present invention. For example, information on the type of rendering application 34 may not be necessary, while additional information about the user and/or the user's computing device 14 may be necessary.

Although Chase teaches specifying the rights description in each license to indicate whether the user has rights to play the digital content, Chase fails to teach or suggest receiving a request to bind a discrete instance of content to a hub network which includes a single server and one or more clients as members of said hub network.

Regarding limitation (e) of claim 1, it recites "enabling a bound instance to bind said discrete locked content data to said hub network at the server as source locked content data". Support for this limitation is found in at least Paragraphs [0032], [0034], and [0039] of the specification of the present application as published in U.S. Pub. No. 2004/0139022 and recited below (emphasis added):

> [0032] As discussed below, an instance that is compliant with hub network operation is in one of two exclusive states: discrete or bound. A discrete instance is independent of any hub network and can be played or presented through any compliant device (according to the license of the discrete instance). However, a compliant device cannot make a usable copy of a discrete instance. A discrete instance includes locked content data and a discrete license. The locked content data of the discrete instance is referred to as the "discrete version" of the locked content data. The locked content data is locked by being protected from unauthorized access, such as by encryption. A bound instance is bound to one hub network. The bound instance is one logical instance represented by locked content data and corresponding licenses stored on the server of the hub network and on zero or more of the clients of the hub network. The locked content data stored by the server is the source for copies of the content data in the hub network and is the "source version." Copies of the source version content data are stored on clients and are "sub-copy

versions" (though some or all of the data in the discrete version, the source version, and/or any of the sub-copy versions can be the same). A bound instance can only be played or presented through a compatible compliant device that is a member of that hub network. Members of that hub network can make sub-copies of the content data of a bound instance.

[0034] In FIGS. 2-16, letter labels indicate the versions of locked content data of instances of content. The version of the locked content data, and so also the state of the instance corresponding to the locked content data, is indicated by variations of the letter. Underlining indicates a discrete version of content. For example, a discrete version of the movie A is indicated by "A". An uppercase letter without underlining indicates a source version of locked content data, stored on a server. For example, the source version of the movie A is indicated by "A". A lowercase letter indicates a sub-copy version of locked content data. For example, a sub-copy version of the movie A is indicated by "a". The versions also have corresponding licenses (not shown in FIGS. 2-16): a discrete version has a discrete license, a source version has a root license, and a sub-copy version has a sub-copy license.

[0039] ... Because the instance stored on the compliant optical disc is compliant and has not been bound to any hub network yet, the instance is a discrete instance. Jim inserts the compliant optical disc into the server device of the car 120 and causes the car 120 to bind the discrete instance of the movie X to the hub network HN2. The car 120 creates a bound instance of the movie X and stores a source version of locked content data and root license as part of the bound instance in the storage of the car 120 and disables the discrete instance on the compliant optical disc (e.g., by storing data to the optical disc). After the discrete instance on the compliant optical disc has been disabled, the discrete version of the locked content data of the disabled instance cannot be played or presented on another device (as described below, in another implementation, when a discrete instance is bound to a hub network, the then-disabled discrete instance can still be played by member devices in the hub network to which the discrete instance was bound). In FIG. 6, the source version of the movie X is

> indicated by the "X" label added to the car 120. Similarly, Jim purchases and downloads a compliant instance of a song Y from network 115 and causes the car to bind the instance to the hub network HN2. In FIG. 6, the source version of the song Y is indicated by the "Y" label added to the car 120.

The Office Action cites to Chase as teaching limitation (e) in paragraphs [0017] and [0212], and states that "digital content **12** is tightly bound to the license **16**; see also para [0017], where a license is bound to a specific black box; see para [0186], where a black box **30** is tightly tied to or associated with the user's computing device **14** and will not render content if transferred to another computing device **14**)". The cited passages are shown below.

> [0017] Importantly, the license server only issues a license to a DRM system that is `trusted` (i.e., that can authenticate itself). To implement `trust`, the DRM system is equipped with a `black box` that performs decryption and encryption functions for such DRM system. The black box includes a public/private key pair, a version number and a unique signature, all as provided by an approved certifying authority. The public key is made available to the license server for purposes of encrypting portions of the issued license, thereby binding such license to such black box. The private key is available to the black box only, and not to the user or anyone else, for purposes of decrypting information encrypted with the corresponding public key. The DRM system is initially provided with a black box with a public/private key pair, and the user is prompted to download from a black box server an updated secure black box when the user first requests a license. The black box server provides the updated black box, along with a unique public/private key pair. Such updated black box is written in unique executable code that will run only on the user's computing device, and is re-updated on a regular basis.
>
> [0186] Preferably, the upgraded black box 30 delivered by the black box server 26 is tightly tied to or associated with the user's computing device 14. Accordingly, the upgraded black box 30 cannot be operably transferred among multiple

> computing devices 14 for nefarious purposes or otherwise. In one embodiment of the present invention, as part of the request for the black box 30 (step 901) the DRM system 32 provides hardware information unique to such DRM system 32 and/or unique to the user's computing device 14 to the black box server 26, and the black box server 26 generates a black box 30 for the DRM system 32 based in part on such provided hardware information. Such generated upgraded black box 30 is then delivered to and installed in the DRM system 32 on the user's computing device 14 (steps 907, 909). If the upgraded black box 30 is then somehow transferred to another computing device 14, the transferred black box 30 recognizes that it is not intended for such other computing device 14, and does not allow any requested rendering to proceed on such other computing device 14.
>
> [0212] It is important to note that the above-specified series of steps represents an alternating or `ping-ponging` between the license 16 and the digital content 12. Such ping-ponging ensures that the digital content 12 is tightly bound to the license 16, in that the validation and evaluation process can only occur if both the digital content 12 and license 16 are present in a properly issued and valid form. In addition, since the same decryption key (KD) is needed to get the content server 22 public key (PU-CS) from the license 16 and the digital content 12 from the package 12p in a decrypted form (and perhaps the license terms (DRL 48) from the license 16 in a decrypted form), such items are also tightly bound. Signature validation also ensures that the digital content 12 and the license 16 are in the same form as issued from the content server 22 and the license server 24, respectively. Accordingly, it is difficult if not impossible to decrypt the digital content 12 by bypassing the license server 24, and also difficult if not impossible to alter and then decrypt the digital content 12 or the license 16.

As stated above, although Chase alludes to content being tightly bound to a license, it fails to teach or suggest enabling a bound instance to bind the discrete locked content data to the hub network at the server as source locked content data.

For at least the above reasons, Chase fails to render unpatentable claim 1.

Because dependent claims inherit the patentability of their respective independent claims, claims 2-6, 9-15, and 71 are not made unpatentable by Chase.

Accordingly, it is submitted that the rejection of claims 1-6, 9-15, and 71 based upon 35 U.S.C. §102(e) has been overcome by the present remarks and withdrawal thereof is respectfully requested.

§103 Rejection of Claims 1-6, 9-15, and 71

In Section 27 of the Office Action, claims 1-6, 9-15, and 71 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Chase in view of Peinado (U.S. Patent Pub. 2002/0013772).

The Office Action alternatively cites to Peinado as teaching "distributing content packages **12p** via magnetic or optical disks or other storage devices (see para [0070]; see also para [0078], where the content ID of digital content **12** is included in the digital content package **12p**)." The Office Action further states that this teaching of Peinado alternatively teaches limitation (c) of claim 1 which states that "the discrete license is not bound to said hub network". Although the applicants disagree with this contention, it is submitted that even assuming arguendo that this content is true, other limitations of claim 1 (as discussed above) provide patentable subject matter for claim 1 over Chase and Peinado.

Accordingly, it is submitted that the rejection of claims 1-6, 9-15, and 71 based upon 35 U.S.C. §103(a) has been overcome by the present remarks and withdrawal thereof is respectfully requested.

§103 Rejection of Claims 7-8 and 16-20

In Section 30 of the Office Action, claims 7-8 and 16-20 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Chase in view of Peinado.

Based on the above discussions, claim 1 should be allowable over the combination of Chase and Peinado. Because dependent claims inherit the patentability of their respective independent claims, dependent claims 7-8 and 16-20 should also be allowable over the combination of Chase and Peinado.

Accordingly, it is submitted that the rejection of claims 7-8 and 16-20 based upon 35 U.S.C. §103(a) has been overcome by the present remarks and withdrawal thereof is respectfully requested.

Conclusion

In view of the foregoing, applicants respectfully request reconsideration of claims 1-20 and 71 in view of the remarks and submit that all pending claims are presently in condition for allowance.

In the event that additional cooperation in this case may be helpful to complete its prosecution, the Examiner is cordially invited to contact Applicant's representative at the telephone number written below.

Please charge any additional fees, including any fees for additional extension of time, or credit overpayment to Deposit Account No. 50-2075.

Respectfully submitted,

Dated: February 16, 2012

By: /Samuel S. Lee/
Samuel S. Lee
Reg. No. 42,791

Procopio, Cory, Hargreaves & Savitch LLP
525 B Street, Suite 2200
San Diego, California 92101-4469
(619) 525-3821